GROUP-IB



Fraud Research

Part 1 of investment scams targeting the United States and Australia

Social Media Pump-and-Dump Investment Scam

How a Social Media Pump and Dump Scheme Exploits Trust Across Australia and the United States

GROUP-IB.COM

Table of contents

01 Disclaimer 03

02 Acknowledgements 05
- Authors 05
- Contributors 05

03 Introduction 06
- Further Reading 07

04 Key findings 07

05 Attribution 08
- Threat Actors 08
- Scam Profiles 09
- Victimology 10

06 Social media pump and dump scheme 11
- Stage 0: Reconnaissance & Resource Development 13
- Stage 1: Initial Lure and Social Engineering 16
- Stage 2: Instant Messenger-Based Engagement and Guided Trading 17
- Stage 3: Cash-Out via Pump & Dump Execution 21

07 Towards a predictive defence: Group-IB's Cyber Fraud Fusion Approach 25
- Scenario 1: Cyber Fraud Fusion Applied to Social Media Pump-and-Dump 26
- Why Cyber Fraud Fusion Matters 27

08 Conclusion 28

09 Recommendations 29
- For Individuals 29
- For Trading Platforms 29
- For Financial Institutions 30
- For the Ecosystem 30

10 Indicators of Compromise (IOCs) 31

01 Disclaimer

01	This report is provided for informational purposes only. The findings, assessments, and recommendations are based on data available at the time of publication and are subject to change as new intelligence emerges.
02	While every effort has been made to ensure the accuracy of the information, Group-IB makes no warranties, express or implied, regarding completeness, reliability, or suitability for any particular purpose.
03	Readers are permitted to download, review, and cite this report for personal or educational use, provided that proper attribution is given to Group-IB and a link to the original source is included. Any commercial use or redistribution of the report without prior written consent from Group-IB is strictly prohibited.
04	This report may reference legitimate third-party services such as WhatsApp, Facebook, and others, solely to illustrate cases where threat actors have abused or misused these platforms. All companies named as victims of impersonation—including EverQuote, Inc.—are legitimate entities not implicated in any fraud.
05	This report is protected under applicable copyright and intellectual property laws. All trademarks referenced herein are the property of their respective owners and are used solely for informational purposes, without any implication of affiliation or sponsorship.
06	Unauthorized reproduction, distribution, or other use of the report, in whole or in part, without written consent from Group-IB, may result in legal action, including claims for damages.
07	All forensic activities described were conducted under client authorization and in compliance with applicable laws. This report is provided for informational and defensive purposes only, and its recommendations must be applied in accordance with legal requirements.
08	This report may reference legitimate and/or legal third-party services solely to illustrate how threat actors misuse or abuse such platforms or services. All trademarks are property of their respective owners.

09	Nothing in this report constitutes investment advice, a recommendation, an offer or a solicitation to buy or sell any security. Any references to specific securities are illustrative only and historical in nature; readers must not rely on them for any investment decision.
10	This report is not investment research within the meaning of any applicable securities laws or regulations and has not been prepared in accordance with legal or regulatory requirements designed to promote the independence of investment research.
11	References to third-party financial institutions, trading platforms, cryptocurrency exchanges or individuals are included for illustrative purposes only. Unless expressly stated otherwise, such references do not imply any involvement, wrongdoing, negligence, liability or compliance failing on the part of those parties, all of which are understood to be themselves subject to abuse by the threat actors described in this report. Where individual names are referenced, those names are treated as aliases or pseudonyms attributed to the threat actor on the basis of observed activity, and do not refer to, or imply any connection with, any real person bearing those names.
12	Indicators of compromise published in this report reflect observations at the time of research and may subsequently have been reassigned, recycled or remediated. Readers should not actively interact with the listed infrastructure and should independently validate any indicator before operationalizing it.
13	Any person or entity referenced in this report who considers that the reference is inaccurate or otherwise warrants review is invited to contact law@group-ib.com within 30 days of publication. The publisher will consider good-faith correction requests on their merits.
14	Unauthorized reproduction, distribution, or other use of the report, in whole or in part, without written consent from Group-IB, may result in legal action, including claims for damages.

02 Acknowledgements

We would like to express our sincere gratitude to all teams whose expertise and dedication made this report possible. This investigation was a collaborative effort led by Group-IB's Fraud Protection team, involving analysts from Investigations, Threat Intelligence, and its Computer Emergency Response Team (CERT-GIB). Their combined work in analyzing, correlating, and contextualizing data played a critical role in uncovering the tactics, techniques, and procedures of the threat actor. This report is a testament to the power of cross-functional collaboration in the face of complex adversarial threats.

Authors



Yuan Huang
Senior Fraud Analyst



Afiq Sasman
Head of CERT-GIB, Asia-Pacific



Aleksandr Sychev
Senior Cyber Investigation Specialist

Contributors



Zafar Astanov
Deputy Head of Fraud & Financial Crime Solutions



Vladimir Kalugin
Operational Director of Group-IB's Unified Products



Dmitry Pisarev
Product Manager, Fraud Intelligence



Nikita Rostovtsev
Technical Head, Attack Surface Management, Threat Intelligence and Digital Risk Protection, Asia-Pacific



Jia Hwei Soh
Head of High Tech Crime Investigations, Asia-Pacific

03 Introduction

Investment scams remain among the most financially damaging forms of fraud affecting individuals in both Australia and the United States. In 2025, the Australian Competition and Consumer Commission (ACCC) reported that Australian consumers suffered a total of US$2.18 billion in scam-related losses across all categories, with investment scams accounting for US$837.7 million — the single highest-loss scam type, representing over a third of all reported losses. In the United States, the U.S. Federal Trade Commission (FTC) reported that consumers in the United States reported US$7.9 billion in losses to investment scams in 2025, with a median individual loss of US$10,000. These figures not only underscore the scale and severity of the problem, but also highlights the increasing sophistication and evolving tactics and techniques used by scammers to lure consumers into such schemes.

Among the most concerning developments in this landscape is the emergence of social media-driven stock manipulation schemes that exploit the credibility of legitimate financial institutions and public figures. Threat actors now deploy deepfake technology to impersonate well-known economists and financial analysts, create geo-targeted advertisements that funnel victims into messenger-based coordination groups, and direct them to purchase specific stocks on real, regulated trading platforms. The manipulation occurs not on the exchange itself, but in the social engineering layer — making detection and attribution exceptionally difficult.

This article—the first in a two-part series on investment scams targeting Australia and the United States—provides a comprehensive examination of this pump-and-dump scheme.

During the course of Group-IB's investigation, our analysts identified more than 20 WhatsApp accounts impersonating a single Australian economist, observed both Australian and US-registered phone numbers operating similar schemes, and documented a real-world case study in which a NASDAQ-listed stock was targeted, and demonstrating that as few as 500 to 3,000 victims can generate sufficient coordinated buying pressure to move a stock price by over 12%.

This report further examines how Group-IB's Cyber Fraud Fusion (CFF) approach, one that unifies Digital Risk Protection, Threat Intelligence, Fraud Protection, Cyber Fraud Intelligence Platform and Investigation capabilities, can detect and disrupt these operations at the point when fraudsters first publish their advertisements on social media,, before coordinated buying inflates stock prices and before victims incur losses.

Further Reading

>200

connected fake cryptocurrency investment platforms

This report is a two-part series focusing on investment scams targeting victims in the United States and Australia.

Please visit Group-IB's Research Hub for part 2 of this series, focusing on fake or unlicensed investment platforms, where we uncover a network of over 200 connected fake cryptocurrency investment platforms with an estimated revenue exceeding $187 million.

04 Key findings

01	Threat actors impersonate well-known financial professionals using deepfake technology and geo-targeted social media advertisements to funnel victims into WhatsApp-based coordination groups.
02	Over 20 fake WhatsApp accounts impersonating a single Australian economist were identified during investigation, suggesting centralised control by an organised group.
03	Both Australian (+61) and US (+1) registered phone numbers were observed operating similar pump-and-dump investment schemes targeting Australian residents, indicating cross-jurisdictional threat actor involvement.
04	Victims are instructed to trade on legitimate, regulated platforms (e.g., MooMoo, CommSec, Interactive Brokers), making the fraud appear as lawful trading activity.
05	Analysis of a NASDAQ-listed stock (EVER) recommended by the threat actor demonstrates that a coordinated inflow of between US$1.5 million to US$3 million, requiring as few as 500 to 3,000 victims, can drive a 12.4% price increase in a small-cap equity.
06	The targeted stock was selected for its "sweet spot" characteristics: moderate daily volume (~300K shares) liquid enough to avoid suspicion yet thin enough for coordinated buying to move the price.

05 Attribution

Threat Actors

Group-IB customers can access our Threat Intelligence portal for more information about the following threat actors below.



Gold Bull

First seen
30 August 2025

About

GoldBull is a financially motivated threat actor engaged in social media–driven pump-and-dump schemes, primarily targeting victims in Australia and the United States. The group leverages impersonation of credible financial professionals to build trust and manipulate individuals into participating in coordinated stock price inflation campaigns.

Skillset

- Social engineering
- Deepfake generation
- Geo-targeted phishing
- Stock manipulation
- Multi-account OpSec

Toolset

- Facebook and Instagram advertisements
- Deepfake tools
- WhatsApp accounts
- Geo-redirect URLs
- Legitimate trading platforms

Targeted Industries

- Financial services
- Retail investment and trading services

Motivation

- Financial gain

Modus Operandi

GoldBull deploys deepfake advertisements that impersonate trusted authorities to build credibility and lure victims. Targets are then funneled through geo-targeted redirects to localized landing points, where they are directed to engage via fraudulent WhatsApp accounts (typically using +61 and +1 numbers). From there, victims receive step-by-step guidance to purchase specific stocks on legitimate trading platforms, enabling the actor to orchestrate a coordinated pump-and-dump scheme for financial gain.

Scam Profile

Group-IB customers can access our Fraud Intelligence portal for more information about the scam profile below.

Social Media Pump-and-Dump

Threat Actors
Gold Bull

First Discovered
Unknown

About

Social media impersonation combined with messenger-based coordination to execute stock price manipulation. Threat actors impersonate financial professionals, coordinate simultaneous buying of small-cap stocks via WhatsApp groups, then sell pre-positioned holdings at inflated prices.

Techniques

- Deepfake advertisements
- Impersonation of public and authoritative figures
- Geo-targeted URL redirection
- WhatsApp-based social engineering
- Coordinated stock options buying
- Proof-of-purchase requirements

Targeted Jurisdictions

- Australia
- United States

Victim Path

01 Social media advertisement (Facebook, Instagram)

02 Geo-targeted redirection

03 WhatsApp contact/group

04 Guided stock purchase on legitimate trading platform

05 Pump-and-dump execution

Victimology

The following data is sourced from the ACCC Targeting Scams Report (2025), the U.S. Federal Trade Commission (FTC) Consumer Sentinel Network (2025), and Scamwatch. Investment scams represent the highest-loss fraud category in both jurisdictions.

By Jurisdiction

Jurisdiction	Industries / Entities Targeted	Reported Losses (2025)
Australia	Individuals (retail investors) · Banking clients · Trading platform users	US$837.7 million (investment scams) US$2.18 billion (all scam types)
United States	Individuals (retail investors) · Banking clients · Trading platform users	US$7.9 billion (investment scams) US$15.9 billion (all fraud types)

By Sector

Sector	Industries / Entities Targeted	Reported Losses (2025)
Trading Platforms	Legitimate regulated platforms abused by threat actors in connection with pump-and-dump activity.	Brand impersonation and reputational risk; indirect losses through client victimisation

In Australia, 481,523 scam reports were filed across all agencies in 2025, with 274,577 involving financial losses. Australians aged 65 and over accounted for 26.5% of total losses reported to Scamwatch. Online-based scams with a financial loss increased by 31.8% in 2025. In the United States, 3 million fraud reports were filed in 2025, with investment scams alone accounting for approximately half of all reported fraud losses.

06 Social media pump and dump scheme

Overview	This scheme combines social media impersonation with instant messenger-based coordination to execute a pump-and-dump stock manipulation. Threat actors impersonate reputable financial professionals and use private messaging groups to coordinate simultaneous buying of small-capitalisation stocks, typically with a market capitalization of between US$300 million to US$2 billion, then sell their pre-positioned holdings at the artificially inflated price.
Jurisdictional Relevance	This scheme has been observed targeting both ASX-listed stocks in Australia and NASDAQ/OTC stocks in the United States. Victims of this scam would be instructed by threat actors to trade on legitimate, regulated platforms, making detection and attribution more complex.

Pump-and-Dump Investment Scam: Attack Chain and Operation Flow

Step 0

Reconnaissance & Resource Development

- Identify target stocks.
- Pre-position holdings in the target stock(s) at low prices
- Create multiple fake social media profiles impersonating public figures.
- Set up fake messenger accounts (e.g. WhatsApp, Telegram) for victim engagement.
- Generate phishing URLs using geo-targeted mechanism.
- Develop marketing collateral such as fake performance screenshots.

Step 1

Initial Lure & Social Engineering

- Victims are attracted by fake investment advertisement on social media platforms.
- Victims click the phishing link and are then connected with TA's WhatsApp accounts.

Step 2

Messenger / WhatsApp-based Engagement & Guided Trading

- Threat actor asks victims to trade in legitimate platforms, and provide trading signal with stock name, limit buying price and target price (selling price).
- Victims are asked to provide screenshot of purchase proof and wait for further instruction.

Step 3

Cash-out via Pump-and-Dump Execution

- The coordinated buying pressure from victims causes the target stock price to increase in the short term (the “pump”) and then the threat actor sells (dumps) their pre-accumulated shares, often before the stock reaches the “target price”.
- The stock price drops dramatically (the “dump”), leaving victims holding overvalued shares at financial loss.

Stage 0 Reconnaissance & Resource Development

Impersonation of Public Figures and Reference to Legitimate Financial Institutions

To establish immediate credibility, threat actors frequently impersonate well-known economists, financial analysts, or staff from reputable online stockbroking firms such as CommSec. They also reinforce legitimacy by referencing trusted and legitimate financial institutions including major Australian banks like the Commonwealth Bank and the National Australian Bank; payment services such as PayPal and fintech platforms; the Australian Securities Exchange (ASX); and global trading platforms like Interactive Brokers.

The tactic of impersonating a public figure is highly persuasive and effective because it exploits pre-existing public trust, thereby lowering victims' scepticism toward subsequent instructions. Referencing recognisable brands gives fraudulent content a veneer of legitimacy, and victims are more likely to engage when familiar institutional names are invoked.

A notable example involves the abuse of the personal brand of a well-known Australian economist and market commentator. Threat actors created fraudulent accounts using his name, likeness, and professional credentials to lend authority to fraudulent investment advice. Artificial intelligence and deepfake technologies were observed being used to generate fake image and video advertisements referencing reputable financial entities.

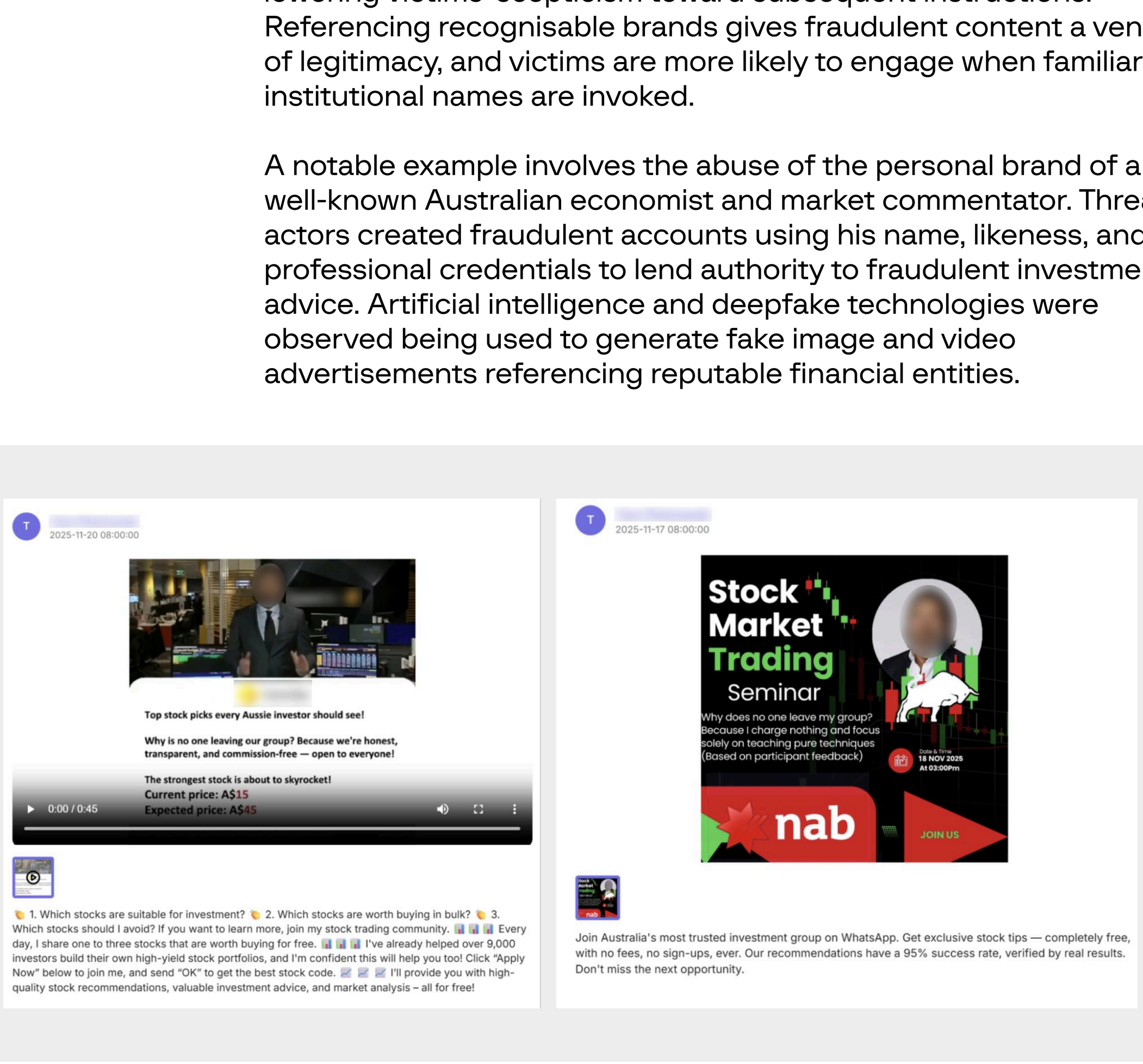


Figure 1. Screenshots of social media posts using the well-known Australian economist's likeness by threat actors in order to exploit their victims' trust.

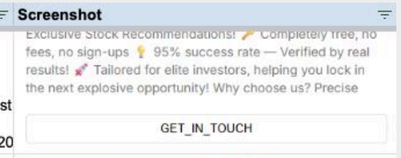
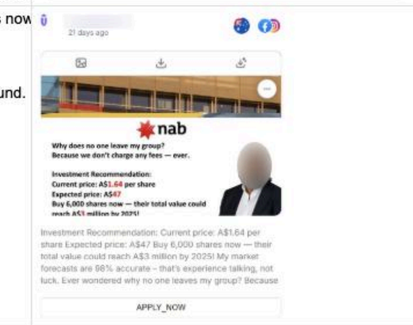
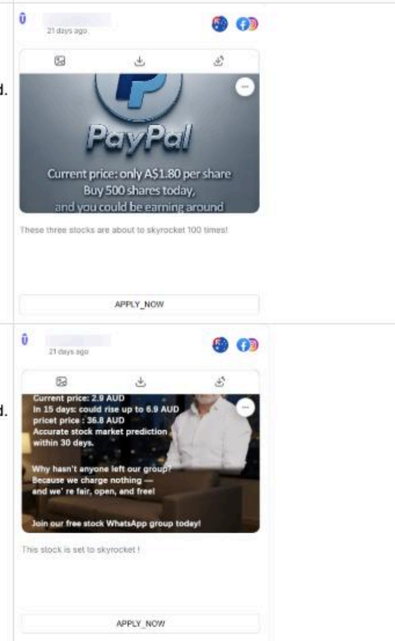
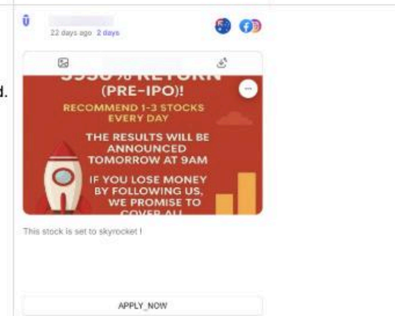
Date of Advert	Persona	Company	FB Page/Profile nam	FB Page/Profile Link	Advert	Screenshot
2025-10-30 7:00:00		Australian Securities Exchange & Commonwealth Bank of Australia		https://www.facebook.com/100089520920	Completely free. No fees, 100% free access to our high-potential stock list. Privacy guaranteed: Your information is securely protected through Facebook ⏳ Don't miss this opportunity! Click to join our WhatsApp group and get the exclusive stock investment list Congratulations! Get in touch with me on WhatsApp, and I'll send you a free list of top stocks to watch in 20	
2025-10-17 7:00:00		National Australia Bank		https://www.facebook.com/100090151807	Investment Recommendation: Current price: A$1.64 per share Expected price: A$47 Buy 6,000 shares now Join our exclusive investor crew and start winning! Only a few spots left! Join our exclusive WhatsApp group and unlock expert investment secrets! This group's been given the tick by Facebook. Your deets are safe as houses and won't be shared around. Got a broking account? YES NO How long ya been trading or investing? Just starting out 1-3 years More than 3 years Email Terms and Conditions for Join now and reply to get your stock list! Nearly there – last step! Hit us up on WhatsApp – I'll shoot ya a free list of top stocks to watch in 2025!	
2025-10-17 7:00:00		PayPal		https://www.facebook.com/100090151807	These three stocks are about to skyrocket 100 times! Join our exclusive investor crew and start winning! Only a few spots left! Join our exclusive WhatsApp group and unlock expert investment secrets! This group's been given the tick by Facebook. Your deets are safe as houses and won't be shared around. Got a broking account? YES NO How long ya been trading or investing? Just starting out 1-3 years More than 3 years Email Terms and Conditions for Join now and reply to get your stock list! Nearly there – last step! Hit us up on WhatsApp – I'll shoot ya a free list of top stocks to watch in 2025!	
2025-10-17 7:00:00		Australian Securities Exchange		https://www.facebook.com/100094022565	This stock is set to skyrocket ! Join our exclusive investor crew and start winning! Only a few spots left! Join our exclusive WhatsApp group and unlock expert investment secrets! This group's been given the tick by Facebook. Your deets are safe as houses and won't be shared around. Got a broking account? YES NO How long ya been trading or investing? Just starting out 1-3 years More than 3 years Email Terms and Conditions for Visit Privacy Policy. Nearly there – last step! Hit us up on WhatsApp – I'll shoot ya a free list of top stocks to watch in 2025!	
2025-10-16 7:00:00		Interactive Brokers		https://www.facebook.com/100094022565	This stock is set to skyrocket ! Join our exclusive investor crew and start winning! Only a few spots left! Join our exclusive WhatsApp group and unlock expert investment secrets! This group's been given the tick by Facebook. Your deets are safe as houses and won't be shared around. Got a broking account? YES NO How long ya been trading or investing? Just starting out 1-3 years More than 3 years Email Terms and Conditions for Visit Privacy Policy. Nearly there – last step! Hit us up on WhatsApp – I'll shoot ya a free list of top stocks to watch in 2025!	

Figure 2. A screenshot of a compilation of sample of advertisements posted by fraudsters on social media impersonating and using the well-known Australian economist's likeness to exploit their victims' trust.

For more information about how threat actors are exploiting artificial intelligence to exploit public trust and impersonation, please refer to Group-IB's Weaponized AI report.

Set up Fake Messenger Accounts and Generate Geo-Targeted Redirection URLs

When victims click the fake advertisement, they are redirected based on their IP address. Australian IP addresses are then routed to add a fake messenger account impersonating a public figure on WhatsApp or Telegram for further victim engagement. IP addresses that do not originate from Australia are routed to blocked pages, or redirected to legitimate investment websites overseas.

The purposes of this geo-targeting approach is threefold: it concentrates on victims within the target geography, reduces international scrutiny, and complicate cross-jurisdictional collaborative investigations.

The following is a list of intermediary redirected links that Group-IB's CERT (GIB-CERT) analyst detected:

None
Intermediary redirected links:
https://75zjzn[.]shop/
https://acnows[.]shop/dblxnT
https://acnows[.]shop/Lo5VNu
https://acnows[.]shop/P3gN9P
https://adsmkop[.]today/
https://dbvlfpf[.]shop/
https://evppqgl[.]today/
https://kfspwsp[.]today/
https://kseffep[.]today/
https://kuylvwr[.]shop/
https://lhsestj[.]shop/
https://mvgbolk[.]today/
https://ncpojhx[.]shop/
https://qervyby[.]today/
https://qtwuiro[.]today/
https://rohssnw[.]today/
https://ssdun[.]cc/3kPnht
https://ssdun[.]cc/D0aIAm
https://ssdun[.]cc/tMmr17
https://tzoinst[.]today/
https://wfhoxat[.]today/
https://yryqbbb[.]today/
https://acnows[.]shop/P3gN9P

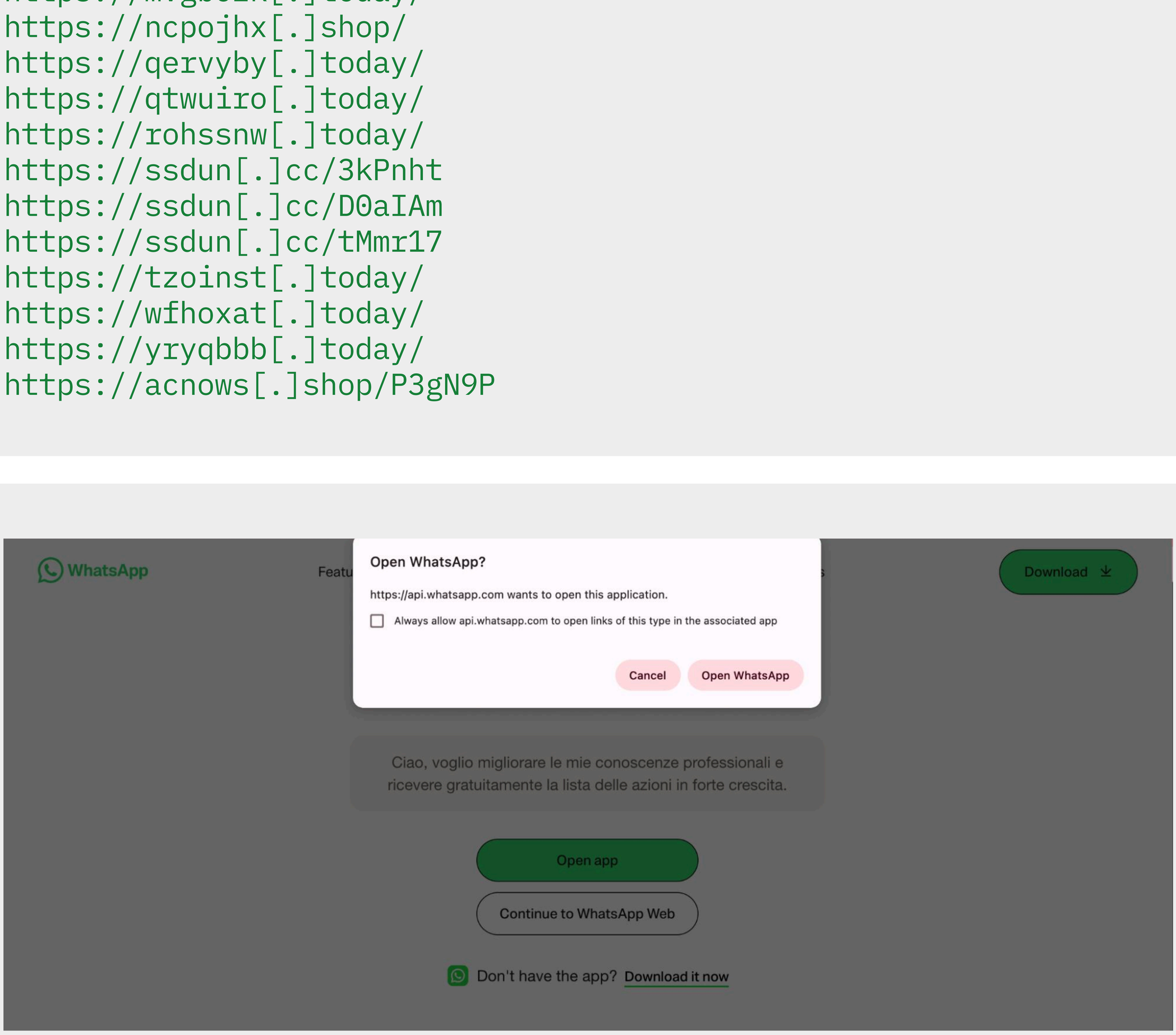


Figure 3. A screenshot of the redirection page to WhatsApp

Stage 1 Initial Lure and Social Engineering

Fake Advertisements on Social Media

With all necessary resources developed, the threat actors post paid advertisements on social media platforms such as Facebook or Instagram as lures to attract potential victims, leveraging the credibility of impersonated financial professionals and institutions. These advertisements promise exclusive stock tips, guaranteed high returns, or insider trading signals to create urgency and capitalizes on their potential victims' fear of missing out (FOMO). Once victims click the advertisement, they are directed to add a WhatApp or Telegram contact belonging to the threat actor, or an invitation to join a private "VIP investment group."

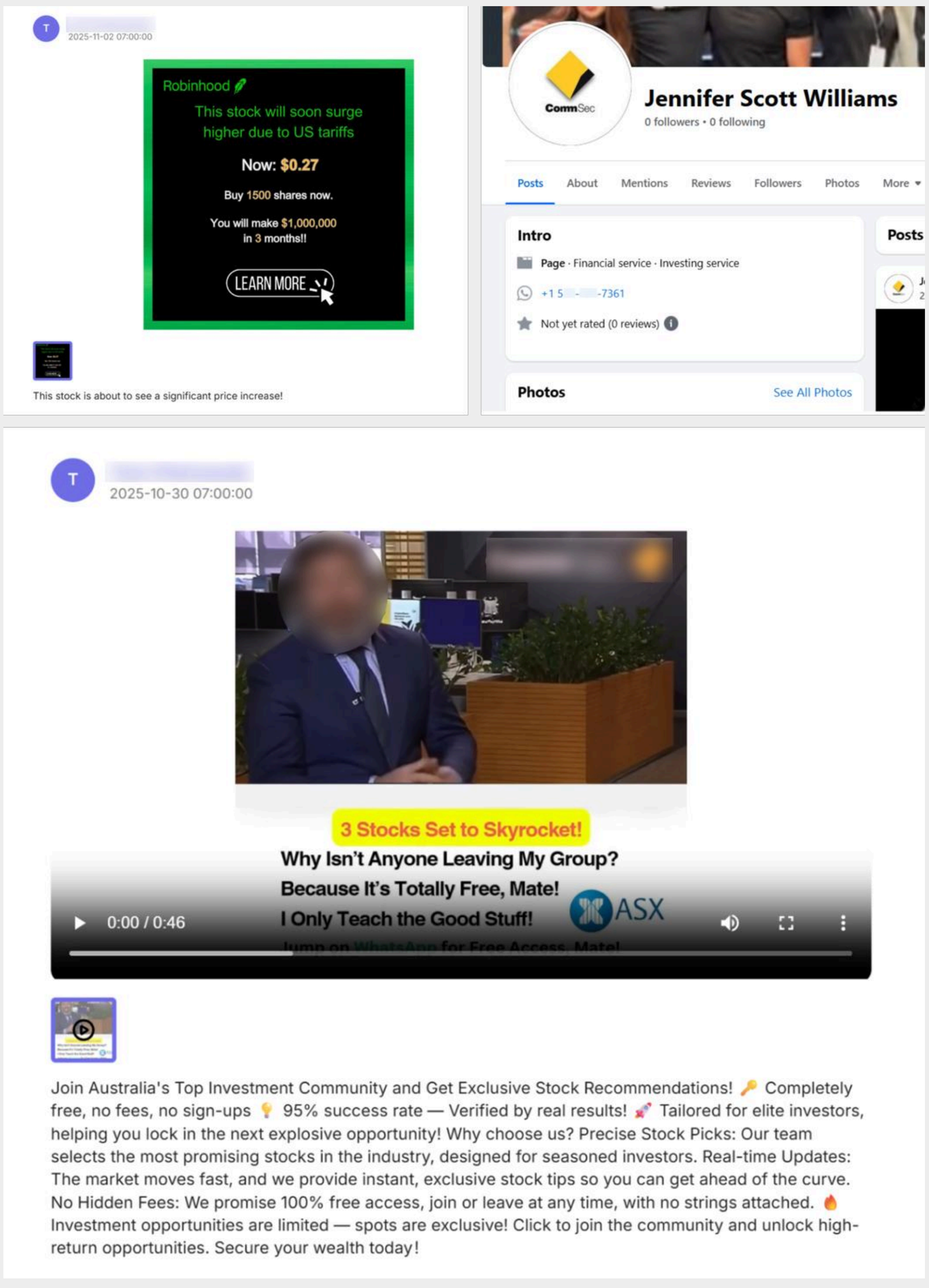


Figure 4. A series of screenshots depicting posts on social media touting stock trading tips and invitations to join a community to receive "exclusive stock recommendations" from the well-known Australian economist and other financial sector figures.

Short Advertisement Lifespan to Evade Detection and Removal

Group-IB has observed that these advertisements typically remain active for brief periods, sometimes only a few hours. This strategy may be employed because social media platforms could detect and remove the suspicious content, or because the threat actors deliberately rotate advertisements to evade detection. In either case, the short exposure window creates artificial urgency for users who encounter the ads.

Stage 2 Instant Messenger-Based Engagement and Guided Trading

Multiple Fake WhatsApp Accounts

Upon clicking on the advertisement via social media, victims are redirected and typically connected with individual contacts first. During the course of Group-IB's investigation, our analyst clicked more than 20 different advertisements and was connected with more than 20 accounts on WhatsApp impersonating the well-known Australian economist. Despite the use of multiple accounts, the coordinated nature of messaging across these accounts suggests centralised control by a single threat actor, or an organised cybercriminal syndicate.

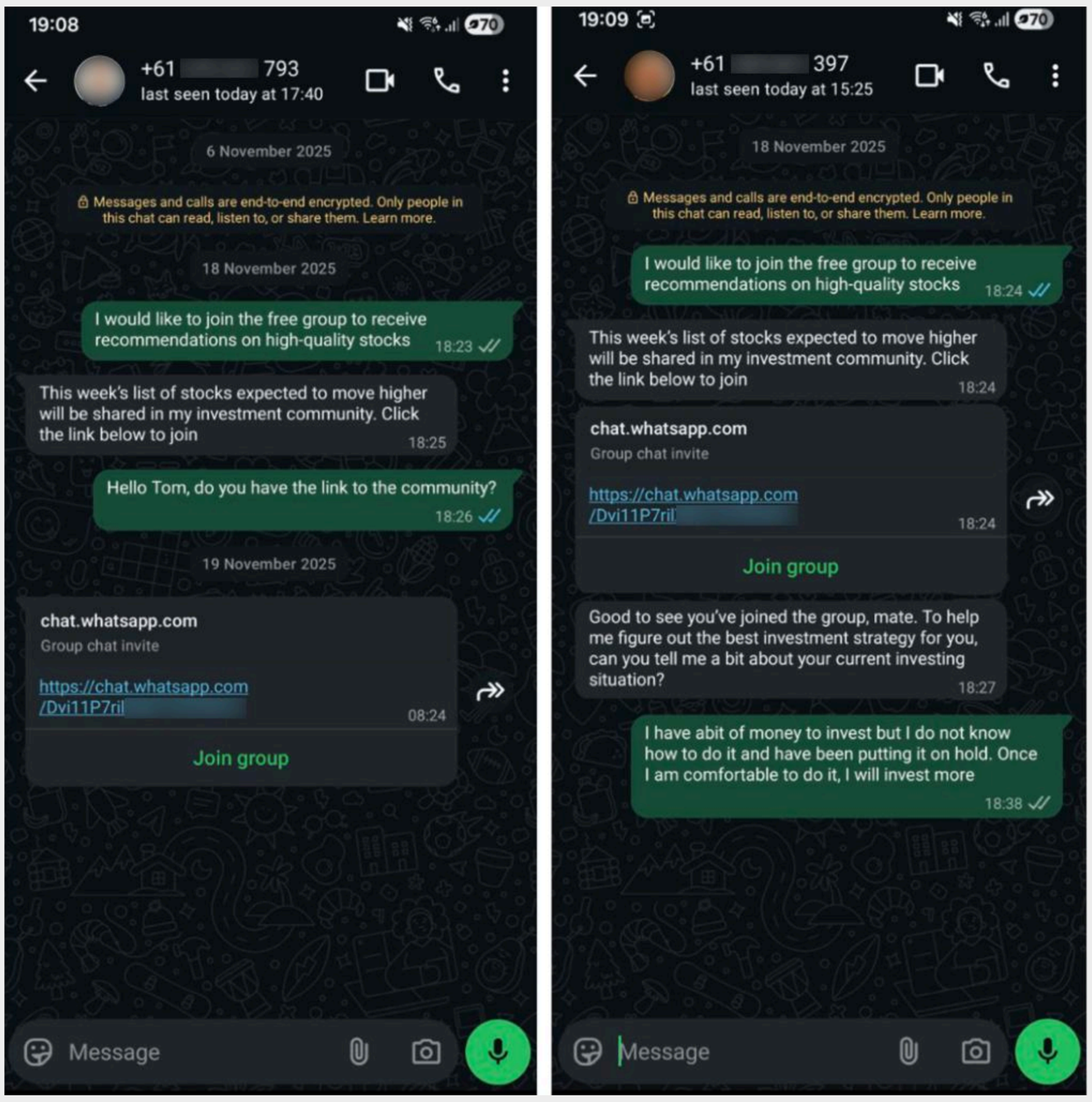


Figure 5. Screenshots of two separate conversations on WhatsApp with different mobile numbers impersonating the well-known Australian economist, with the same text and links from the sender (threat actor).

The following is a list of Fake Piotrowski WhatsApp accounts that was detected by Group-IB:

```
None
Fake Piotrowski WhatsApp accounts:
https://api[.]whatsapp.com/send/?
phone=61424207236&text=Get+instant+information+about+high-
quality+stocks&type=phone_number&app_absent=0
https://api[.]whatsapp.com/send/?
phone=61426353160&text=Get+instant+information+about+high-
quality+stocks&type=phone_number&app_absent=0
https://api[.]whatsapp.com/send/?
phone=61469333142&text=Get+instant+information+about+high-
quality+stocks&type=phone_number&app_absent=0
https://api[.]whatsapp.com/send/?
phone=61469382365&text=Get+instant+information+about+high-
quality+stocks&type=phone_number&app_absent=0
https://api[.]whatsapp.com/send/?phone=61469872315&text=Get+high-
quality+stock+market+information%21&type=phone_number&app_absent=0
https://api[.]whatsapp.com/send?
phone=61415805623&text=Get%20premium%20stock%20information%20now!
https://api[.]whatsapp.com/send?
phone=61433006761&text=I%20would%20like%20to%20join%20the%20free%2
0group%20to%20receive%20recommendations%20on%20high-
quality%20stocks.
https://api[.]whatsapp.com/send?
phone=61469816770&text=I%20would%20like%20to%20join%20the%20free%2
0group%20to%20receive%20recommendations%20on%20high-
quality%20stocks.!
https://api[.]whatsapp.com/send?
phone=61469841397&text=I%20would%20like%20to%20join%20the%20free%2
0group%20to%20receive%20recommendations%20on%20high-
quality%20stocks!
https://api[.]whatsapp.com/send?
phone=61469841397&text=I%20would%20like%20to%20join%20the%20free%2
0group%20to%20receive%20recommendations%20on%20high-
quality%20stocks.
https://api[.]whatsapp.com/send?
phone=61469841397&text=I%20would%20like%20to%20receive%20today%27s
%20information%20about%20that%20soaring%20stock!
https://api[.]whatsapp.com/send?
phone=61470227571&text=Get%20premium%20stock%20information%20now!
https://api[.]whatsapp.com/send?
phone=61470227571&text=Get%20premium%20stock%20information%20now!
https://api[.]whatsapp.com/send?
phone=61470321793&text=I%20would%20like%20to%20join%20the%20free%2
0group%20to%20receive%20recommendations%20on%20high-
quality%20stocks.
```

```
https://api[.]whatsapp.com/send?
phone=61470321793&text=I%20would%20like%20to%20join%20the%20free%2
0group%20to%20receive%20recommendations%20on%20high-
quality%20stocks.
```

WhatsApp Group Dynamics

During our investigations, one of our analyst was added to a WhatsApp group that touted such investment schemes, but was quickly removed then after. This indicates that the group maintains a high level of operational security and anti-detection awareness. Within these WhatsApp groups, threat actors pose as "head analysts" or "senior advisors", regularly sharing specific stock recommendations daily, or every few days. These recommendations would often include precise entry prices (limit buy prices) and target exit prices. Victims would also be instructed to purchase the recommended stock through their own legitimate trading platforms, for example MooMoo, or Interactive Brokers.

Australian and US Registered Phone Numbers

Group-IB observed that all of the WhatsApp accounts impersonating the well-known Australian economist used to run these WhatsApp groups utilized the **+61 country code**, indicating the use of Australian-registered phone numbers.

However, US-registered phone numbers **(+1 country code)** were also observed during our investigation, indicating that threat actors operating from the US, or elsewhere using US-registered phone numbers, may also be involved in investment fraud targeting Australia.

For example, after clicking on a phishing advertisement claiming affiliation with CommSec, (the largest online stockbroking platform in Australia) on Facebook, our analyst was connected with a WhatsApp account +1 (5XX) XXX-7361, associated with a WhatsApp profile named “Laura Taylor” but linked to a Facebook account under the name “Jennifer Scott Williams”.

There is currently no evidence to determine whether the Australian and US-registered phone numbers are linked to the same or different threat actor groups. However, their behavioural patterns demonstrate a similar pump-and-dump fraud scheme.

Example Case:

Interaction with Individual WhatsApp Threat Actor

Through interactions with the persona “Jennifer Scott Williams” (aka Laura Taylor) while posing as a prospective investor, our analyst identified a common victim engagement pattern. The threat actor typically begins by asking how long the victim has been investing and how much capital they are willing to commit. After establishing this baseline, they instruct the victim to deposit funds on a legitimate trading platform (e.g., MooMoo, CMC) and wait for a trading signal. A signal is shared shortly thereafter, specifying the stock name, a limit buying price, and a target selling price. Victims are asked to provide a screenshot as proof of purchase and to wait for further instructions and tailored trading plans.

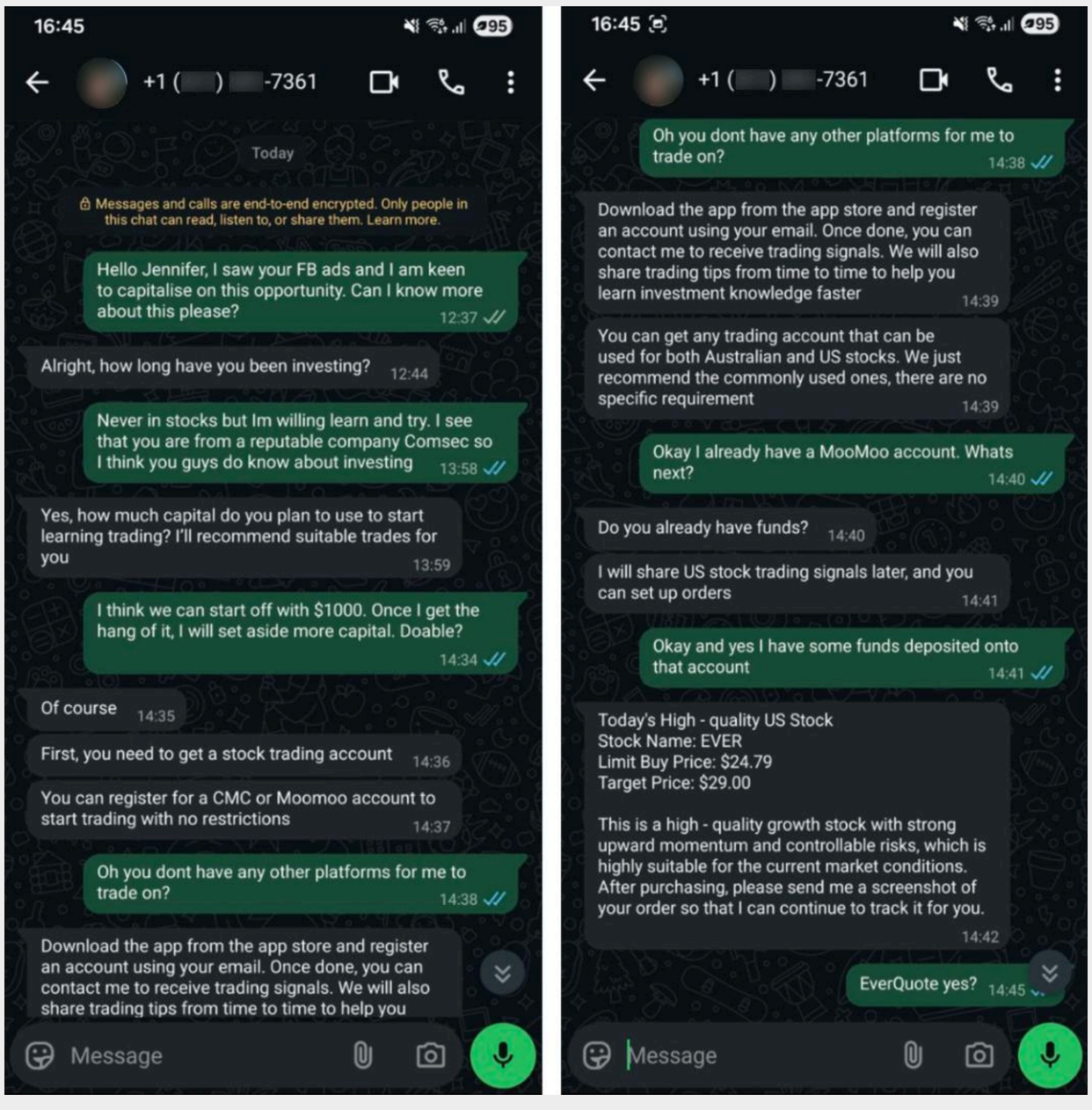


Figure 6. Interactions between Group-IB’s Fraud Protection analyst and the “Jennifer Scott Williams” (aka Laura Taylor) persona via WhatsApp.

Stage 3 Cash-Out via Pump & Dump Execution

How Threat Actors Profit from Pumping and Dumping

Coordinated buying by victims drives a short-term increase in the target stock’s price ("pumping"). The threat actor then sells (“dumping”) their pre-accumulated shares at the inflated price, often before the stock reaches the "target price" communicated to victims.

After the threat actor exits their position and coordinated buying subsides, the stock price typically drops dramatically (the "dump"), leaving victims holding overvalued or near-worthless shares and incurring significant financial loss. The threat actor may attribute the decline to "market conditions" and attempt to redirect victims to a new stock to repeat the cycle. In some cases, threat actors may also take short positions after the pump phase to profit from the subsequent price decline.

The Observed Timeline of the Recommended Stock (EVER)

During the engagement with “Jennifer Scott Williams” (aka Laura Taylor) persona via WhatsApp (Figure 5), our analyst was instructed to purchase stocks of EverQuote Inc. (NASDAQ: EVER) at an entry price of US$24.79 per share on November 6, 2025, with a target selling price of US$29.00 per share. The following is a series of stock charts via Interactive Broker that illustrates the real price movement of EverQuote, Inc in March 2026.

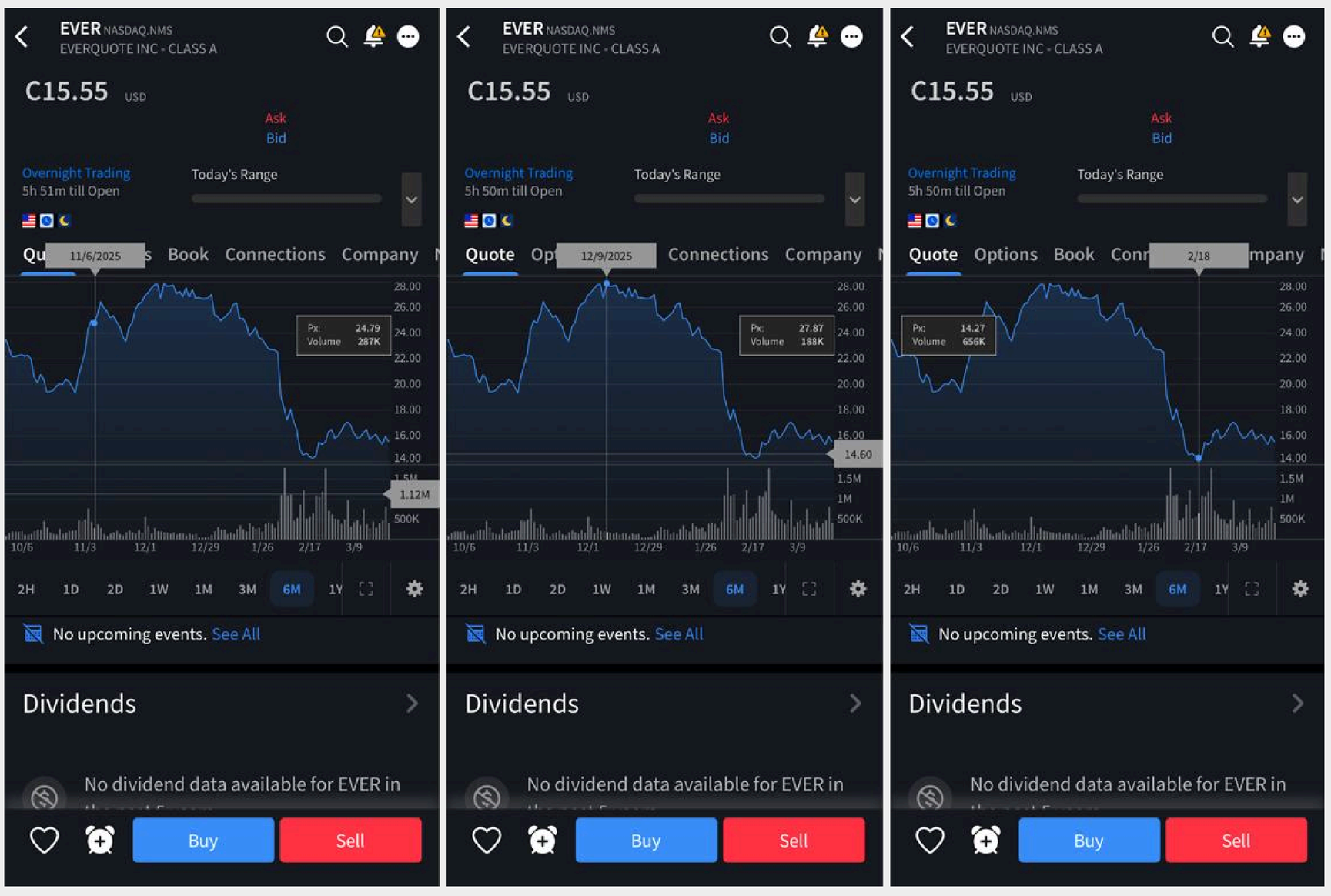


Figure 7. Price movement of EverQuote, Inc in March 2026.

Timeline	Price	Observation
6 November 2025	US$24.79	+ Threat actor instructs victims to buy EVER at US$24.79 via WhatsApp. + Target sell price communicated as US$29.00 (~17% gain). + Victims are asked to provide proof of purchase.
9 December 2025	US$27.87	+ Coordinated buying pressure from other victims contributes to upward price movement. + Stock reaches its local peak of US$27.87 (+12.4% from entry) but does **NOT** reach the promised target of US$29.00.
10-29 December 2025	~US$26–US$27	+ Stock begins declining from its peak.
1 January - 18 February 2026	~US$26 → US$14.27	+ Stock enters steep decline and reaches its lowest point at US$14.27 (–42.4% from entry, –48.8% from Dec 9 peak). + Victims who followed the threat actor's instructions and waited for the US$29 target price suffered devastating losses.

Note: this decline may be also influenced by legitimate market factors, including the launch of competitors' products or broader trade and tariff concerns.

Overestimating the Difficulty of Executing Pump-and-Dump Fraud

Taking the targeted stock (EVER) recommended by the threat actor as an example: EVER had a market capitalisation of approximately US$873 million (at entry ~US$24.79) on November 6, 2025, with an average daily trading volume of around 300,000 to 330,000 shares per day (~US$7.4M daily dollar volume). The following analysis estimates the number of victims and coordinated capital required to move EVER's stock price by 5%, 10%, and 15% from the entry point of US$24.79.

Estimated Coordinated Capital Required to Move EVER Price

Target Increase	Target Price	US$/Share Move	Est. Capital (Low)	Est. Capital (High)	% of Daily US$ Vol.
5%	US$26.03	+US$1.24	US$500,000	US$1,000,000	7–14%
10%	US$27.27	+US$2.48	US$1,000,000	US$2,000,000	14–27%
15%	US$28.51	+US$3.72	US$2,000,000	US$4,000,000	27–54%
12.4% (Actual)	US$27.87	+US$3.08	~US$1,500,000	~US$3,000,000	~20–40%

Estimated Number of Victims Required by Investment Amount

Investment/ Victim	5% (US$500K–US$1M)	10% (US$1M–US$2M)	15% (US$2M–US$4M)	12.4% (US$1.5M–US$3M)
US$1,000	500–1,000	1,000–2,000	2,000–4,000	1,500–3,000
US$2,500	200–400	400–800	800–1,600	600–1,200
US$5,000	100–200	200–400	400–800	300–600
US$10,000	50–100	100–200	200–400	150–300
US$25,000	20–40	40–80	80–160	60–120

The analysis demonstrates that this type of pump-and-dump operation is entirely feasible with a relatively small number of victims. The observed 12.4% price increase (from US$24.79 to US$27.87) could have been achieved with an estimated US$1.5M–US$3M in coordinated buying from victim of the fraud. At US$1,000 per victim, this equates to approximately 1,500–3,000 participants, well within the reach of organised scam groups operating multiple WhatsApp or Telegram chat groups promoting this investment scam.

At higher per-victim investments (US$5K–US$10K), which is common among engaged victims as few as 150–600 victims could generate sufficient buying pressure. A single well-run WhatsApp group holds up to 1,024 members, meaning just two to three groups would be sufficient to coordinate the required buying pressure.

Why EverQuote Inc Was Targeted

EverQuote Inc (NASDAQ: EVER) presents an attractive target for pump-and-dump operators for several reasons:

- It is a legitimate, NASDAQ-listed company with real revenue (~US$692M in FY2025) and analyst coverage, lending credibility to the "tip"

- Its moderate daily volume (~300K shares, ~US$7.4M/day) represents a "sweet spot" for manipulation — **liquid enough that buying activity does not appear immediately suspicious, yet low enough that a coordinated inflow of US$500K–US$2M can meaningfully influence the price**

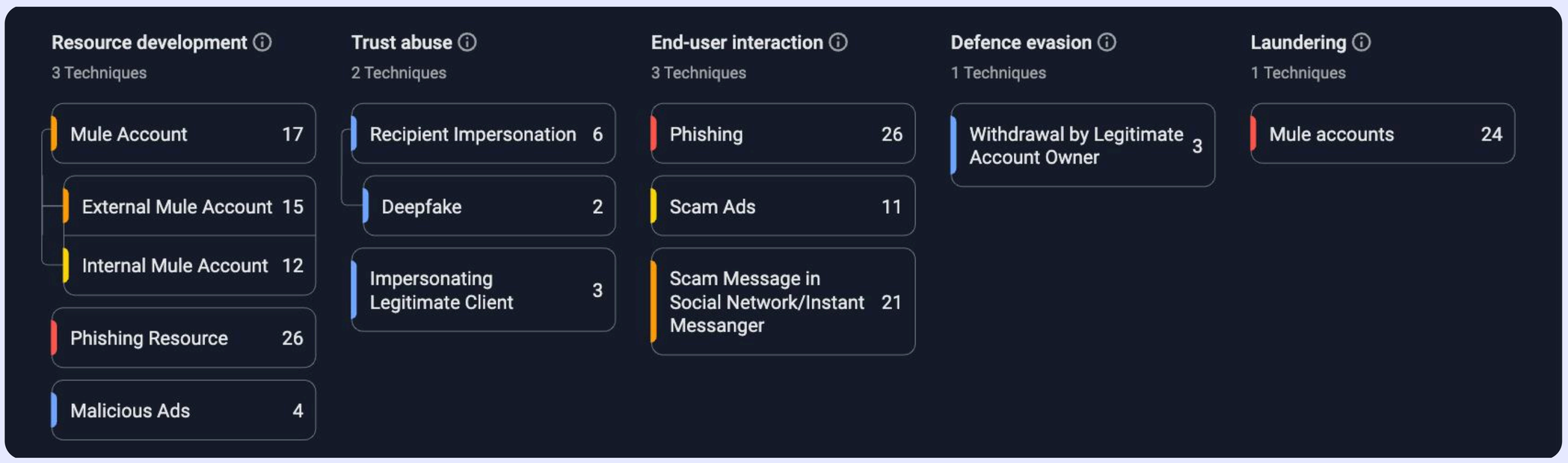
- The stock had positive analyst sentiment (consensus "Strong Buy" with price targets of US$27–US$40 at the time), which could be cited as "validation" of the threat actor's recommendation.

Important Caveats and Disclaimers

This case study presents an analytical assessment based on observed price movements and known scam typologies. It does not constitute evidence of market manipulation by any specific individual or entity in relation to EVER.

EverQuote, Inc. is a legitimate company with real revenue (**US$692.5M in FY2025)**, institutional ownership (~91.5%), and active analyst coverage. The company itself is not implicated in any fraud. This document is prepared for fraud intelligence purposes only and should not be distributed externally without appropriate review.

Fraud Matrix



07

Towards a predictive defence: Group-IB's Cyber Fraud Fusion Approach

The investment scam schemes examined in this fraud research report reveal a critical structural challenge: the attack chains span multiple platforms, jurisdictions, and industries, while the defensive capabilities of individual organisations remain siloed. Banks often have limited visibility into activity on social media. Trading platforms may struggle to detect coordinated actions within messaging groups. While some institutions do monitor social media and messaging platforms, these efforts are typically fragmented and do not provide a complete, end-to-end view of a fraud or scam case.

Group-IB's Cyber Fraud Fusion approach addresses this gap by unifying cybersecurity capabilities including Threat Intelligence (TI), Digital Risk Protection (DRP), and Investigation services, with fraud prevention capabilities such as Fraud Protection and the Cyber Fraud Intelligence Platform (CFIP) into a single coordinated framework. Rather than responding to investment scams after victims have lost money, Cyber Fraud Fusion enables the ecosystem to predict and disrupt operations at the earliest stages of the attack chain, before they reach scale.

The following scenarios illustrate how Cyber Fraud Fusion would operate against the fraud scheme examined in this article, with specific reference to the findings of this research.

Scenario 1 Cyber Fraud Fusion Applied to Social Media Pump-and-Dump

In a pump-and-dump operation, the attack chain proceeds through social media advertisements, messenger-based coordination, guided trading on legitimate platforms, and eventual stock price collapse. Group-IB's Cyber Fraud Fusion would intervene across this chain as follows:

Step 1

Detection — Digital Risk Protection (DRP)

- DRP detects the impersonation of the well-known Australian economist and CommSec branding in social media advertisements and phishing URLs.
- Graph analysis of linked resources reveals the full network of fraudulent ads, geo-targeted redirection URLs, and associated WhatsApp contact numbers — before they are widely distributed.
- DRP initiates automated takedown of the phishing advertisements, reducing the window of victim exposure from hours to minutes.

Step 2

Intelligence Enrichment — Threat Intelligence (TI)

- The TI team analyses the threat actor infrastructure — Australian and US-registered phone numbers, WhatsApp coordination patterns, the specific stocks being promoted, and the timing of campaigns.
- This intelligence is then enriched with dark web monitoring for any references to coordinated pump-and-dump operations or stock manipulation services.

Step 3

Ecosystem Alert — Fraud Protection & CFIP

- The Fraud Protection team shares the alert in real time through CFIP to member institutions — banks and trading platforms such as MooMoo, CommSec, Interactive Brokers, and Stake.
- CFIP members are warned that a specific stock (e.g., EVER) is being promoted through fraudulent channels.
- Trading platforms can flag or alert clients attempting to buy the targeted stock in response to unofficial recommendations, or detect unusual coordinated buying patterns consistent with pump-and-dump activity.

Step 4

Attribution — Investigation Services

- Group-IB's investigation team works to identify the real individuals behind the WhatsApp accounts and social media profiles, building an evidence package to support law enforcement action.

Outcome

In this scenario, the campaign would be disrupted at the advertisement stage, before coordinated buying inflates the stock price and before victims incur losses. In the case of EVER, where the observed price movement of 12.4% was driven by an estimated US$1.5 million toUS$3 million in coordinated buying from between 500 to 3,000 victims, early detection and takedown of the fraudulent advertisements could have have increased operational costs for threat actors, reduced their ROI, and lowered the likelihood of continued operations—thereby preventing the majority of this activity.

Why Cyber Fraud Fusion Matters

The critical insight of the Group-IB's Cyber Fraud Fusion approach is that investment scam operations have **multiple interdependent points of vulnerability** — fraudulent advertisements, messenger coordination and exploitation of legitimate platforms. No single product or team can address all of these simultaneously. However, when DRP detects the initial brand abuse, TI maps the infrastructure and financial flows, CFIP distributes alerts across the financial ecosystem, and Investigation traces funds to real identities, the combined effect is a defence that operates at the speed and scale of the attack itself.

Traditional approaches to investment fraud are reactive.They identify and report incidents after funds have been lost. Group-IB's Cyber Fraud Fusion reverses this dynamic by correlating risk signals across the entire attack chain in real time, enabling the ecosystem to act at the earliest stage of detection rather than the latest stage of loss.

08 Conclusion

The pump-and-dump scheme examined in this article reveals a common and critical characteristic of modern investment fraud: fraudsters do not target technical security — they target and exploit trust. By impersonating respected financial professionals through deepfake technology, leveraging the credibility of legitimate stockbroking firms, and directing victims to trade on real, regulated platforms, these schemes succeed by positioning themselves precisely where trust already exists and redirecting it.

The feasibility analysis is sobering: the barrier to executing a pump-and-dump on a real exchange-listed stock is far lower than most people assume. Two to three WhatsApp groups, 500 to 3,000 victims, and $1.5 million to $3 million in coordinated buying pressure are sufficient to move the price of a NASDAQ-listed stock by over 12%. Existing controls — regulatory warnings, platform moderation, consumer education — are necessary but demonstrably insufficient against an adversary that combines deepfake technology, social media reach, and messenger-based coordination into a scalable, repeatable operation.

A new approach is required. The Cyber Fraud Fusion framework — unifying detection, intelligence, fraud prevention, and investigation under a single coordinated approach — enables the ecosystem to disrupt these campaigns at the advertisement stage, before coordinated buying inflates stock prices and before victims incur losses. The architecture of deception is sophisticated. The architecture of defence must be more so.

09 Recommendations

The scale and sophistication of these schemes demand responses tailored to each stakeholder group within the financial ecosystem.

For Individuals

- Verify any investment platform or advisor's credentials through official regulatory registers: ASIC Connect for Australian entities, and SEC EDGAR / FINRA BrokerCheck for US firms.
- Be sceptical of unsolicited stock recommendations, particularly when received via social media or messaging applications — no legitimate advisor distributes stock tips through WhatsApp groups.
- Research any recommended stock independently before investing, and be wary of stocks promoted with precise entry and exit prices through unofficial channels. Remember: no one can reliably predict the market, and anyone claiming otherwise is selling something other than insight.
- Report suspected scams to Scamwatch (AU), ASIC (AU), the FTC (US), SEC (US), or local law enforcement.

For Trading Platforms

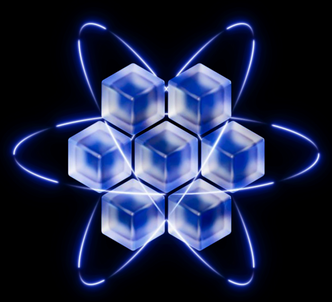
- Detection of pump-and-dump activity presents particular challenges when victims trade on legitimate, regulated platforms.
- The trades themselves appear lawful — the manipulation occurs in the coordination layer (messenger groups) rather than on the platform.
- Trading platforms should consider implementing anomaly detection for unusual coordinated buying patterns in small-cap stocks, particularly when buying activity coincides with social media promotional campaigns.
- Specific indicators include: sudden spikes in buy orders for a stock from clients with no prior trading history in that equity; clusters of buy orders at identical limit prices within a narrow time window; and correlated account activity from clients who recently registered or became active after a period of dormancy.
- Collaboration with social media platforms and regulatory bodies to share intelligence on suspected manipulation campaigns is essential.

For Financial Institutions

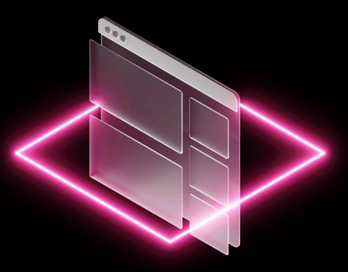
- Actively monitor for brand impersonation across social media, domain registrations, and mobile app stores — particularly the misuse of institutional branding (e.g., CommSec) in fraudulent advertisements.
- Implement alert mechanisms for clients who may be transferring funds to trading accounts in response to social media-promoted stock recommendations.
- Share threat intelligence on identified impersonation campaigns with industry peers and regulators.
- Invest in targeted customer education campaigns that specifically address pump-and-dump mechanics, rather than relying on generic fraud warnings.

For the Ecosystem

Group-IB's Cyber Fraud Fusion approach, as detailed in this article, provides the operational framework for the cross-platform intelligence sharing that the current threat landscape demands. Specific capabilities that would strengthen the collective defence include:



Cyber Fraud Intelligence Platform (CFIP): Real-time, privacy-preserving exchange of anonymised risk signals between banks, trading platforms, and regulatory bodies. When a specific stock is identified as being promoted through fraudulent channels, CFIP enables every participating institution to warn clients and flag suspicious buying patterns simultaneously. CFIP's patented Distributed Tokenisation technology ensures that all customer data remains anonymised, enabling collaboration without compromising privacy compliance.



Digital Risk Protection (DRP): Automated detection and takedown of deepfake advertisements, impersonation profiles, and geo-targeted phishing URLs. DRP's graph analysis can expand a single detection into the full network of connected fraudulent resources, enabling mass enforcement. DRP's continuous monitoring of social media, search engine results, domain registrations, and messenger platforms ensures that fraudulent infrastructure is identified at the earliest possible stage.



Threat Intelligence (TI) and Investigation Services: Analysis of threat actor infrastructure — phone numbers, WhatsApp coordination patterns, targeted stocks, campaign timing — enriched with dark web monitoring for references to stock manipulation services. Identification of the real individuals behind WhatsApp accounts and social media profiles through forensic infrastructure analysis and coordination with law enforcement.

10 Indicator of Compromise (IOCs)

Intermediary redirected links:

https://75zjzn[.]shop/
https://acnows[.]shop/dblxnT
https://acnows[.]shop/Lo5VNu
https://acnows[.]shop/P3gN9P
https://adsmkop[.]today/
https://dbvlfpf[.]shop/
https://evppqgl[.]today/
https://kfspwsp[.]today/
https://kseffep[.]today/
https://kuylvwr[.]shop/
https://lhsestj[.]shop/
https://mvgbolk[.]today/
https://ncpojhx[.]shop/
https://qervyby[.]today/
https://qtwuiro[.]today/
https://rohssnw[.]today/
https://ssdun[.]cc/3kPnht
https://ssdun[.]cc/D0aIAm
https://ssdun[.]cc/tMmr17
https://tzoinst[.]today/
https://wfhoxat[.]today/
https://yryqbbb[.]today/
https://acnows[.]shop/P3gN9P

Impersonation WhatsApp accounts:

https://api[.]whatsapp.com/send/?phone=61424207236&text=Get+instant+information+about+high-quality+stocks&type=phone_number&app_absent=0
https://api[.]whatsapp.com/send/?phone=61426353160&text=Get+instant+information+about+high-quality+stocks&type=phone_number&app_absent=0
https://api[.]whatsapp.com/send/?phone=61469333142&text=Get+instant+information+about+high-quality+stocks&type=phone_number&app_absent=0
https://api[.]whatsapp.com/send/?phone=61469382365&text=Get+instant+information+about+high-quality+stocks&type=phone_number&app_absent=0
https://api[.]whatsapp.com/send/?phone=61469872315&text=Get+high-quality+stock+market+information%21&type=phone_number&app_absent=0
https://api[.]whatsapp.com/send?phone=61415805623&text=Get%20premium%20stock%20information%20now!
https://api[.]whatsapp.com/send?phone=61433006761&text=I%20would%20like%20to%20join%20the%20free%20group%20to%20receive%20recommendations%20on%20high-quality%20stocks.
https://api[.]whatsapp.com/send?phone=61469816770&text=I%20would%20like%20to%20join%20the%20free%20group%20to%20receive%20recommendations%20on%20high-quality%20stocks.!
https://api[.]whatsapp.com/send?phone=61469841397&text=I%20would%20like%20to%20join%20the%20free%20group%20to%20receive%20recommendations%20on%20high-quality%20stocks!
https://api[.]whatsapp.com/send?phone=61469841397&text=I%20would%20like%20to%20join%20the%20free%20group%20to%20receive%20recommendations%20on%20high-quality%20stocks.
https://api[.]whatsapp.com/send?phone=61469841397&text=I%20would%20like%20to%20receive%20today%27s%20information%20about%20that%20soaring%20stock!
https://api[.]whatsapp.com/send?phone=61470227571&text=Get%20premium%20stock%20information%20now!
https://api[.]whatsapp.com/send?phone=61470321793&text=I%20would%20like%20to%20join%20the%20free%20group%20to%20receive%20recommendations%20on%20high-quality%20stocks.
https://api[.]whatsapp.com/send?phone=61470321793&text=I%20would%20like%20to%20join%20the%20free%20group%20to%20receive%20recommendations%20on%20high-quality%20stocks.

GROUP-IB

Group-IB is a creator of cybersecurity technologies to investigate, prevent and fight digital crime.

1,600+
Successful investigations of high-tech crime cases

500+
Employees

60
Countries

$1 bln+
Saved by our client companies through our technologies

#1*
Incident Response Retainer vendor

*According to Cybersecurity Excellence Awards

11
Unique Digital Crime Resistance Centers

Global partnerships

- INTERPOL
- EUROPOL
- AFRIPOL

Recognized by top industry experts

- Forrester®
- datos INSIGHTS
- kuppingercole ANALYSTS
- Gartner®
- IDC
- FROST & SULLIVAN

Fight against cybercrime



GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785